TP-Link Patches Multiple Vulnerabilities in NC Cloud Cameras

TP-Link has released firmware updates to address several vulnerabilities in its NC series cloud cameras, including bugs that could lead to the remote execution of arbitrary commands.

Tracked as CVE-2020-12111, the first of the command injection flaws impacts the NC260 and NC450 models and could be abused to remotely execute commands as root on affected devices.

The issue was identified in the *httpSetEncryptKeyRpm* method (handler for */setEncryptKey.fcgi*) of the *ipcamera* binary, where the user-controlled *EncryptKey* parameter was used directly as part of the executed command line, without input sanitization.

An attacker looking to exploit the vulnerability would need to send an authenticated POST request to */setEncryptKey.fcgi*. This allows them to inject commands in the *EncryptKey* parameter, resulting in those commands being executed with root privileges.

The second command injection bug, CVE-2020-12109, impacts TP-Link NC200, NC210, NC220, NC230, NC250, NC260, and NC450 cloud cameras.

The issue was found in the *swSystemSetProductAliasCheck* method, which is called when a new alias for the device is set via */setsysname.fcgi*, and exists because there are no checks in place to prevent shell metacharacters from being introduced.

Because of this issue, the system name could be used in *swBonjourStartHTTP* as part of a shell command meant to inject arbitrary commands that would then be executed as root.

In addition to these two vulnerabilities, TP-Link addressed a hardcoded encryption key issue in NC200, NC210, NC220, NC230, NC250, NC260, and encryption key issue in NC200, NC210, NC220, NC230, NC250, NC260, and NC450 device models.

Tracked as CVE-2020-12110, the vulnerability is located in the methods *swSystemBackup* and *sym.swSystemRestoreFile*, which use the hardcoded encryption key to encrypt and decrypt a config backup file (using the DES ECB algorithm, with modified s-boxes and permutation tables).

By exploiting this vulnerability, attackers could decrypt backup files and access sensitive data, including details such as alarm FTP server user and password, WLAN passphrase, PPPOE user and password, alarm SMTP server user and password, DDNS user and password.

Security researcher Pietro Oliva, who discovered the vulnerabilities, also notes that the issue could allow an attacker to forge encrypted backup files that can be restored via the web interface to write or overwrite arbitrary files. Thus, the attacker could cause permanent damage or execute code as root.

While almost every camera model uses a different hardcoded key, these keys are easy to find and all devices of the same model share the same encryption key, without providing users with the option to change it.

Firmware updates that address all of these vulnerabilities were released on April 29. Users are advised to install them as soon as possible to ensure that they remain protected.

Related: Apple Awards Researcher $75,000 for Camera Hacking Vulnerabilities

Related: Critical Flaw Exposes TP-Link Wi-Fi Extenders to Remote Attacks

Related: Researchers Replace IP Camera Feed With Fake Footage

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire: